(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 562 278**

(51) Int. CI.:

G06F 21/83 (2013.01)
G07F 19/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.09.2011 E 11180554 (5)**

(97) Fecha y número de publicación de la concesión europea: **11.11.2015 EP 2431899**

(54) Título: **Dispositivo de protección y procedimiento correspondiente**

(30) Prioridad:

15.09.2010 FR 1057387

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2016

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

ROSSI, LAURENT y
SCHANG, BERNARD

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo de protección y procedimiento correspondiente

1. Campo de la invención

La presente invención se refiere al campo de la mejora de la seguridad de dispositivos de pago.

Más en particular, la presente invención se refiere a un dispositivo que permite detectar la inclusión, en un dispositivo de pago, de equipos que tienen por objetivo la obtención fraudulenta de datos confidenciales, tales como datos bancarios.

Numerosos dispositivos permiten a usuarios abonar compras. Más en particular, se han generalizado los dispositivos de pago que utilizan tarjetas bancarias tales como tarjetas chip o tarjetas de banda magnética. Estos dispositivos se denominan generalmente terminales de pago y permiten abonar compras de manera simple y rápida. Otros dispositivos también utilizan las tarjetas chip o de banda: se trata, por ejemplo, de terminales bancarios tales como cajeros automatizados o distribuidores automáticos de billetes. En lo sucesivo, se denomina terminales de pago al conjunto de estos dispositivos, que comprenden a la vez un teclado de entrada y un lector de tarjeta de memoria.

Una de las características de estos terminales de pago es su instalación en el exterior. Más exactamente, estos terminales se instalan en muchos casos en el exterior, para que los usuarios puedan tener acceso a los servicios de pago fuera de horarios de apertura estándar o para permitir a los usuarios efectuar las operaciones que deseen más fácil y más rápidamente (operación de pago, operación de consulta de saldo bancario, operación de transferencia).

De este modo, es frecuente y muy común que estos terminales, de los que los clientes se fían plenamente, se hallen instalados en entornos más o menos inadecuados, habida cuenta de los datos que se manipulan en las operaciones de pago o en operaciones de consulta.

En efecto, la instalación de los terminales de pago en exterior ha hecho que surja un tipo de fraude denominado “collar marsellés”. En este tipo de fraude, se instala un teclado falso por encima del teclado original del terminal de pago (se trata del overlay “teclado”). El distribuidor automático o el cajero automatizado deniega entonces liberar la tarjeta que se ha insertado en él.

Otra técnica, denominada el “skimming”, consiste en instalar, sobre la ranura de introducción de un terminal, un dispositivo que sirve para decodificar la pista magnética o para grabar los datos del chip de la tarjeta bancaria (se trata del overlay “ranura”). La implantación de tal dispositivo en la ranura de introducción de la tarjeta viene muchas veces acompañada de la implantación de un teclado falso (overlay “teclado”) o de la implantación de una cámara que permite filmar el código confidencial del portador de tarjeta en el momento en que el terminal de pago solicita este código. Los datos leídos por este dispositivo fraudulento son transmitidos directamente a los perpetradores de fraude mediante la utilización de un módulo GSM que transmite los datos a un terminal móvil GSM por mediación de un mensaje de tipo SMS/MMS. Los perpetradores de fraude codifican nuevamente o copian los datos en una tarjeta virgen de la que pueden servirse.

2. Soluciones de la técnica anterior

Todos los proveedores de terminales de pago y un cierto número de proveedores terceros están en condiciones de proporcionar soluciones anti-skimming más o menos eficaces. Un equipo de ensayos europeo (European ATM Security Team) ha establecido y mantiene una base de datos de soluciones anti-skimming y de sus funcionalidades. No obstante, actualmente no existen certificaciones o evaluaciones independientes de estas soluciones, y hay algunas soluciones más eficaces que otras.

Así, se han propuesto numerosas soluciones para mitigar estos problemas de seguridad planteados por los terminales de pago, cuando están instalados en entornos poco seguros. Entre estas soluciones cabe citar la modificación del terminal, por ejemplo modificando la forma del terminal. Esta modificación de forma se traduce en la inclusión de volúmenes específicos que impiden engancharle o pegarle un dispositivo fraudulento de lectura de los datos bancarios.

Sin embargo, la eficacia de esta solución es muy relativa. Y es que los fabricantes de dispositivos fraudulentos de lectura de los datos bancarios generalmente fabrican estos dispositivos de manera casera y saben adaptarse a las restricciones específicas de los terminales en los que tienen que adaptarse los dispositivos. Por lo tanto, para los fabricantes de dispositivos fraudulentos de lectura de los datos bancarios es muy simple modificar la forma de sus dispositivos en función de los terminales de pago.

Otra solución que se ha propuesto consiste en dotar el terminal de sensores de presión, en determinados lugares del terminal. Estos sensores de presión presumiblemente captan la inclusión de un dispositivo fraudulento de lectura de los datos bancarios.

Una vez más, la adaptabilidad que demuestran los fabricantes de dispositivos fraudulentos no permite asegurar una

total fiabilidad de esta solución.

Consiste otra solución en dotar el terminal de pago de un dispositivo interferente que perturba la transmisión de datos emitidos desde un ocasional dispositivo fraudulento. Otra solución consiste en dotar el teclado de una guarda específica que se encarga de que el código confidencial introducido por el portador de la tarjeta bancaria no pueda ser grabado, en el tecleo, por una cámara disimulada al lado o sobre el terminal de pago.

La patente FR 2857113, que se refiere al campo de la invención, describe una caja segura que da cabida a un teclado que permite introducir datos confidenciales, tales como un número de identificación personal, destinados particularmente a un sistema de pago electrónico seguro en los aspectos mecánico, electrónico y emisión electromagnética. Esta incluye una matriz táctil capacitiva unida, por una parte, mediante hilos de enlace, a una placa de circuito impreso portadora del asociado controlador, un módulo de seguridad así como una electrónica sensible a las variaciones de capacidad del sistema y, por otra, dispuesta de manera intercalada entre dos placas de vidrio, a saber, una placa de vidrio anterior o placa de protección y una placa de vidrio posterior o placa soporte. El problema de la solución que aporta la patente FR 2857113 está, por una parte, en que no es de aplicación a la implantación de teclado mecánico (el teclado protegido en la patente FR 2857113 es un teclado digital, presentado en una pantalla táctil). Por otra parte, el sistema del documento FR 2857113 no permite solucionar los problemas relacionados con la colocación de un sistema en la ranura del terminal de pago. Por último, la solución que propone la patente FR 2857113 es costosa y compleja en su puesta en práctica.

La solicitud de patente WO 2009/103594 da a conocer un teclado que tiene una pluralidad de teclas y una pluralidad de elementos capacitivos que están asociados a unas ubicaciones de teclas. Sin embargo, la disposición de la pluralidad de elementos capacitivos es complicada y precisa de una modificación de configuración del circuito impreso.

La solicitud de patente US 2008/278355 concierne a un dispositivo de detección capacitivo destinado a equipar los PED (PIN Entry Device). Este dispositivo está equipado con un detector con forma de rejilla, que se ubica alrededor de las teclas del PED. La solución que aporta la solicitud US 2008/278355 no permite detectar los dispositivos intrusos ubicados lateralmente entre las teclas. Es, además, complicada y costosa en su puesta en práctica.

A esta fecha, ninguna solución ha permitido solucionar totalmente este problema, a un coste que se estime razonable. Ahora bien, es importante proporcionar terminales de pago en los que puedan confiar los usuarios, terminales que no por ello sean demasiado onerosos de producir.

3. Sumario de la invención

La invención no presenta los inconvenientes del estado de la técnica. En efecto, la invención concierne a un dispositivo de protección de un terminal de pago electrónico y a un procedimiento de protección de un terminal. Estos objetos se llevan a la práctica tal y como se describen en las reivindicaciones. En las reivindicaciones dependientes se describen otras particularidades de la invención.

De este modo, la invención permite notar la inclusión de dispositivos fraudulentos en el terminal de pago. En efecto, una de las características de los equipos fraudulentos, cualquiera que sea su forma, está en que comprenden una cantidad nada desdeñable de metal y de materiales conductores. Por lo tanto, la inclusión de dispositivos fraudulentos conlleva modificación de la cantidad de carga eléctrica almacenada para un potencial eléctrico dado, potencial que es, dentro del ámbito de la invención, el detector capacitivo dispuesto en las ubicaciones predefinidas.

Así, esta invención mejora la seguridad del terminal de pago y, más en particular, protege más eficazmente contra los ataques conocidos llamados “overlay” o “collar marsellés” del terminal de pago.

Permite luchar eficazmente contra la implantación de dispositivos fraudulentos sobre el teclado y/o sobre la ranura de inserción de tarjeta chip con el propósito de perpetrar fraude.

4. Descripción detallada de la invención

4.1 Descripción de una forma de realización

Consiste el principio de la invención en llevar a la práctica una detección de una modificación excesiva de capacidad eléctrica en el interior del terminal de pago.

Así, la invención propone detectar una modificación de la capacidad (es decir, una modificación de la carga eléctrica) contenida en uno o varios detectores capacitivos dispuestos en ubicaciones particulares dentro del terminal de pago: bajo el teclado y en la ranura de introducción de la tarjeta.

Para conseguir esto, el dispositivo según la invención comprende al menos un detector capacitivo dispuesto entre una placa soporte de las teclas del teclado mecánico del terminal de pago y un soporte definitorio de los puntos de presión de las teclas del teclado. Este detector capacitivo comprende una capacidad determinada previamente y conocida por un microprocesador de medida capacitiva, unido eléctricamente al detector capacitivo y configurado

para detectar una variación de capacidad del detector capacitivo. El dispositivo comprende asimismo medios de transmisión de una información representativa de variación de capacidad, cuando un valor absoluto de una diferencia entre una capacidad medida, en un momento dado, y la capacidad de referencia excede de un umbral también predeterminado.

El detector capacitivo va simplemente implantado bajo las teclas del teclado mecánico. Por lo tanto, la implantación del detector capacitivo es una operación simple y económica, que no precisa de la construcción de una estructura de soporte o de un dispositivo particular.

El detector capacitivo se caracteriza, en una primera forma de realización, por una forma adaptada a una implantación entre los orificios que permiten el accionamiento de las teclas del teclado bajo el cual se aloja, tal y como se describe con relación a la figura 1.

Más en particular, la figura 1 describe un circuito impreso multicapa 10 (también denominado PCB) sobre el cual se disponen unos componentes electrónicos 11 que pueden ser de montaje superficial (CMS) o soldados al circuito impreso.

Sobre el circuito impreso 10 se ubica asimismo un elemento de soporte mecánico inferior 12 que contiene los elementos de opresión sobre los puntos de presión de las teclas del teclado. Este soporte se monta sobre el circuito impreso en la fabricación del terminal. De acuerdo con la invención, el detector capacitivo 13 se implanta sobre el elemento de soporte mecánico 12. El detector capacitivo 13 va unido eléctricamente al microprocesador de medida capacitiva (no representado). En el montaje del terminal de pago, la placa soporte de las teclas del teclado 14, que constituye el elemento de soporte mecánico superior 14, oculta el detector capacitivo 13 el cual, de este modo, queda invisible tanto a usuarios autorizados como a perpetradores de fraude.

De acuerdo con la invención, el detector capacitivo 13 tiene la forma general de un rastrillo (13-1) que comprende una pluralidad de dientes (13-2 a 13-9). Más en particular, se caracteriza por el hecho de que está configurado para conformarse a la ubicación de las teclas del teclado. Más en particular, la forma del detector capacitivo 13 se define de manera tal que los dientes (13-2, 13-9) no obstruyen los orificios del elemento de soporte mecánico 12 de los puntos de presión (ya se trate de los orificios de las verdaderas teclas o de teclas falsas, destinadas a poner en práctica otra medida de protección del terminal). En efecto, al ser cada vez más las medidas adoptadas para proteger los terminales, es necesario, para que el terminal funcione correctamente, que no interfieran los dispositivos de protección insertos en el seno de los terminales.

De acuerdo con otra característica de la invención, el detector capacitivo 13 comprende además un diente complementario (13-10) destinado, cuando el terminal de pago en cuyo seno se ensambla el dispositivo de la invención, a quedar posicionado paralelamente a la ranura de introducción 15 de la tarjeta (tarjeta de pago, tarjeta de acceso, etc.). Esta característica permite, con un solo detector capacitivo 13, cumplir a la vez la función de detección de implantación de teclado falso y a la vez la función de detección de implantación de lector de tarjetas falso. De este modo, no es necesario prever dos detectores capacitivos. Puesto que un solo soporte basta para cumplir las dos funciones, no es necesario además prever dos calibraciones diferentes, lo cual facilita aún más la puesta en práctica del dispositivo con respecto a los dispositivos de la técnica anterior, por lo que reduce su coste.

4.2 Parametrización inicial

Para poder prestar el servicio esperado, se debe parametrizar el dispositivo de la invención con el fin de determinar el valor predeterminado de la capacidad de referencia. Esta capacidad de referencia permite, como ya se ha aclarado, controlar la variación de capacidad a lo largo del tiempo y determinar si esta variación excede de un valor predeterminado.

Con la primera puesta en tensión del terminal de pago en cuyo seno va montado el dispositivo de la invención, se realiza una medida de calibración y una parametrización con el fin de identificar el valor de referencia, en reposo en un entorno electromagnético neutro, de la capacidad del detector capacitivo.

En lo sucesivo, esta calibración inicial establece la capacidad de referencia. En modo de funcionamiento estándar, por supuesto se admite una variación de la capacidad medida con respecto a la capacidad de referencia, para permitir un funcionamiento normal del terminal de pago.

Un valor llamado “delta” fija los límites superiores e inferiores dentro de los cuales se consideran válidas las capacidades medidas. Las medidas se efectúan periódicamente, bien a intervalos regulares, o bien en horarios predefinidos (tal como, por ejemplo, por la noche).

En efecto, los presentes inventores han comprobado que los fraudes mediante la implantación de dispositivos fraudulentos generalmente se efectúan en periodos temporales cortos (por ejemplo, el teclado falso y el dispositivo de lectura de tarjetas): del orden de media hora. Semejante práctica por parte de los perpetradores de fraude se explica por el hecho de que los perpetradores de fraude se hallan con frecuencia físicamente presentes en una zona muy próxima a aquella donde está instalado el terminal de pago objetivo del fraude, y de que es necesario que

puedan intervenir rápidamente en ese terminal. De este modo, para no ser advertidos, la duración del fraude es, muchas veces, restringida.

Para poder contrarrestar el fraude, es pues necesario realizar las medidas en los momentos en los que es susceptible de tener lugar el fraude. De este modo, cabe asimismo la posibilidad de configurar el dispositivo para definir unos márgenes de medidas adaptados a la localización final del terminal de pago. Por ejemplo, si se trata de una estación de servicio, las medidas se realizarán mejor por la noche, de manera repetida o continuamente, ya que es por la noche cuando el terminal de pago se deja sin vigilancia.

En caso de corte de la alimentación eléctrica procedente de la red eléctrica, los órganos de seguridad del terminal siguen funcionando a batería. En este caso, un sistema de letargo y de despertar periódico del procesador "capacitivo" permite una medida regular de los detectores capacitivos (como por ejemplo, cada 500 milisegundos).

En efecto, el dispositivo de la invención, puesto que consume muy poca corriente eléctrica, se puede llevar a la práctica sin la presencia de una alimentación eléctrica procedente de la red eléctrica. De este modo, el sistema de la invención puede asumir la seguridad del terminal de manera continua con la presencia de la corriente de red eléctrica o sin ella.

Bajo algunas condiciones estrictas, un sistema de compensación ambiental puede modificar el valor de referencia (Baseline). Tal sistema se puede incorporar al dispositivo de la invención para encargarse de un correcto funcionamiento del terminal de pago en función del entorno en el que está instalado.

Se efectúa también un filtrado lógico para discriminar los eventos que, modificadores de las líneas de campo, no son verdaderas colocaciones de dispositivos fraudulentos (manipulaciones del terminal, etc.).

Todas las medidas están pilotadas por mediación de un microprograma asociado al microprocesador de medida capacitiva.

Con relación a la figura 2, se presenta una forma de realización de un terminal de pago según la invención.

Tal terminal comprende una memoria 21 constituida a partir de una memoria intermedia, una unidad de procesamiento 22, equipada, por ejemplo, con un microprocesador P y pilotada por el programa de ordenador 23, que lleva a la práctica el procedimiento de protección según la invención.

Con la inicialización, las instrucciones de código del programa de ordenador 23 se cargan, por ejemplo, en una memoria RAM, antes de ser ejecutadas por el procesador de la unidad de procesamiento 22. La unidad de procesamiento 22 recibe como entrada al menos una información I, tal como identificadores de zonas de localización. El microprocesador de la unidad de procesamiento 22 lleva a la práctica las etapas del procedimiento de protección anteriormente descrito, según las instrucciones del programa de ordenador 23, para suministrar una información procesada T, tal como la detección de un ataque que conlleva la eliminación de los datos protegidos. Para ello, el terminal comprende, además de la memoria intermedia 21:

- al menos un detector capacitivo dispuesto entre un elemento de soporte mecánico inferior de un teclado de dicho terminal y un elemento de soporte mecánico superior de dicho teclado de dicho terminal, estando configurado dicho al menos un detector para suministrar una capacidad de referencia;
- un microprocesador de medida capacitiva unido eléctricamente a dicho al menos un detector capacitivo, configurado para detectar una variación de capacidad de dicho al menos un soporte de medida capacitiva;
- medios de transmisión de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia excede de un umbral predeterminado.

Estos medios están pilotados por el microprocesador de la unidad de procesamiento.

REIVINDICACIONES

1. Dispositivo de protección de un terminal de pago electrónico, comprendiendo el dispositivo:

- al menos un detector capacitivo (13) dispuesto entre un elemento de soporte mecánico inferior (12) de un teclado de dicho terminal y un elemento de soporte mecánico superior (14) de dicho teclado de dicho terminal, estando configurado dicho al menos un detector para suministrar una capacidad de referencia;

- un microprocesador de medida capacitiva unido eléctricamente a dicho al menos un detector capacitivo (13), configurado para detectar una variación de capacidad de dicho al menos un detector capacitivo (13);

- medios de transmisión de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia excede de un umbral predeterminado,

estando conformado dicho detector capacitivo (13) de modo que se extienda entre unos orificios de dicho elemento de soporte mecánico inferior (12),

estando caracterizado dicho dispositivo de protección por que dicho detector capacitivo (13) tiene la forma general de un rastrillo (13-1) que comprende una pluralidad de dientes (13-2 a 13-9).

2. Dispositivo de protección según la reivindicación 1, caracterizado por que además comprende medios de calibración que suministran dicha capacidad de referencia.

3. Dispositivo según la reivindicación 1, caracterizado por que dicho detector capacitivo (13) comprende además un diente complementario (13-10) que, cuando el terminal de pago en cuyo seno se ensambla el dispositivo de la invención, queda posicionado paralelamente a la ranura de introducción de tarjeta en el seno de dicho terminal.

4. Procedimiento de protección de un terminal de pago electrónico que comprende al menos un circuito impreso (10), un dispositivo de protección y una caja, comprendiendo dicho dispositivo de protección:

- al menos un detector capacitivo (13) dispuesto entre un elemento de soporte mecánico inferior (12) de un teclado de dicho terminal y un elemento de soporte mecánico superior (14) de dicho teclado de dicho terminal, estando configurado dicho al menos un detector para suministrar una capacidad de referencia;

- un microprocesador de medida capacitiva unido eléctricamente a dicho al menos un detector capacitivo (13), configurado para detectar una variación de capacidad de dicho al menos un detector capacitivo (13);

- medios de transmisión de una información representativa de dicha variación de capacidad, cuando un valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia excede de un umbral predeterminado,

estando conformado dicho detector capacitivo (13) de modo que se extienda entre unos orificios de dicho elemento de soporte mecánico inferior (12), teniendo dicho detector capacitivo (13) la forma general de un rastrillo (13-1) que comprende una pluralidad de dientes (13-2 a 13-9),

estando caracterizado dicho procedimiento de protección por que comprende al menos una iteración de las siguientes etapas:

- medida de una capacidad actual con el concurso de dicho detector capacitivo (13);

- cálculo de dicho valor absoluto de una diferencia entre dicha capacidad medida y dicha capacidad de referencia;

- transmisión de dicha información representativa de dicha variación de capacidad, cuando dicho valor absoluto excede de dicho umbral predeterminado.

5. Procedimiento según la reivindicación 4, caracterizado por que además comprende, en una primera puesta en tensión de dicho terminal de pago electrónico, una etapa de calibración de dicho terminal que suministra dicha capacidad de referencia.

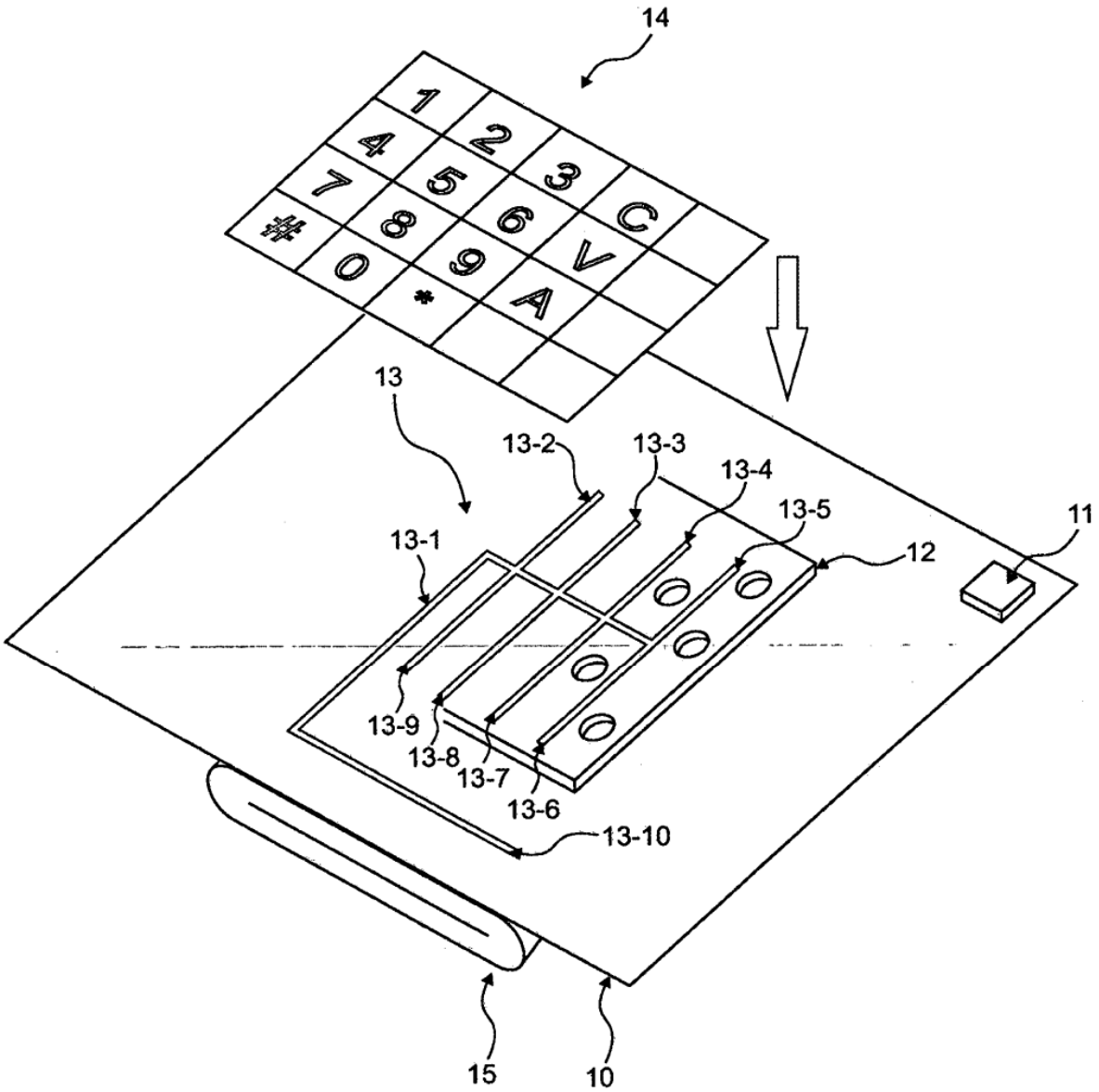
14
1
2
3
C
4
5
6
V
7
8
9
A
#
0
*
13
13-1
13-2
13-3
13-4
13-5
12
11
13-9
13-8
13-7
13-6
13-10
15
10

Fig. 1

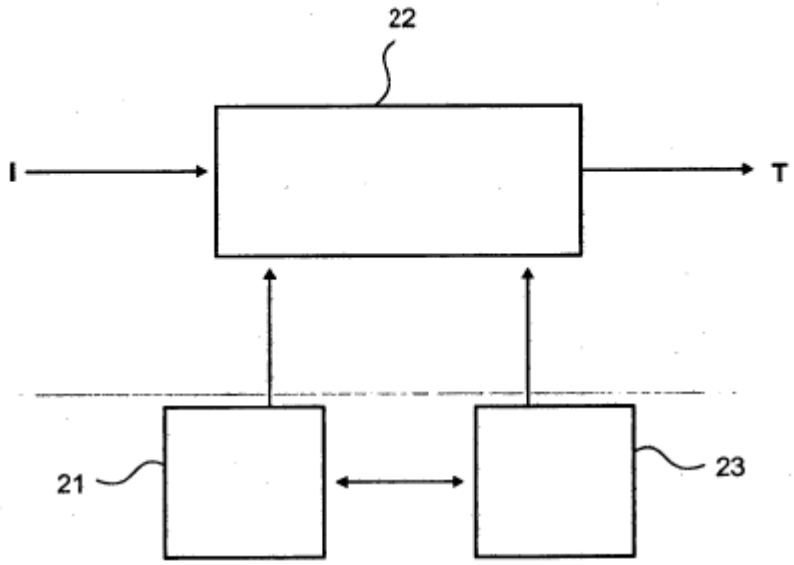

Fig. 2